

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**STIPULATION OF
EXPECTED TESTIMONY**

Mr. Jacob Grant

DATED: 10 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. Jacob Grant were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I currently serve as Contract Task Lead for CCJ6, assigned to the Active Cyber Defense Branch at U.S Central Command's Headquarters (USCENTCOM) on MacDill Air Force Base (AFB) in Florida. In this capacity, I am responsible for conducting various levels of Cyber Operations for USCENTCOM and Overseas Areas of Responsibility (AOR)—including Computer Network Defense (CND) activities, Computer Network Attack (CNA) planning & analysis, and the analysis and reverse engineering of Computer Network Exploitation (CNE) activities in order develop effective countermeasures. I am the lead for our “in-house” Computer Emergency Response Team (CERT). In this capacity, I perform in-depth forensic analysis of CND alerts, flow analysis, or interpretation of threat information to include security compromises, network intrusions, and malicious logic outbreaks. I have held this position for four and a half years. At the time of my involvement in this case, I was the Senior INFOSEC Analyst with the Information Assurance (IA) Branch of the J6 USCENTCOM. I have also been an IA Watch Officer, a Senior Analyst, and a Senior Engineer. I served for two years as an enlisted Airman working in technical control and network engineering.

2. I am a Certified Information Systems Security Professional (CISSP) (2008). I have a Top Secret/SCI security clearance. I have Associates degrees in Electronic Systems Technology and Avionics Systems Technology. I am a Cisco Certified Network Associate (CCNA) (2003) and a CORE Impact Certified Professional (CICP) (2013). Some of the network security and associated training I have received includes: McAfee Network Security Platform Administration (2013), ArcSight ESM Use Case Foundations (2012), EnCase Computer Forensics 1 (2012), ArcSight Logger 5.0 Administration and Operations (2011), Basic Malware Analysis Using Responder Professional (2010), Ethical Hacking (2008), McAfee Host-Based Security Systems (2007), Information Technology Service Management (ITSM) (2007), and Cisco Securing Networks w/ PIX & ASA (SNPA) (2007).

3. I became involved in this case for two reasons. From 19-20 August 2010, I was involved in the collection and transfer of audit logs from the USCENTCOM SharePoint on the USCENTCOM SIPRNET web server. At this time, I was also involved in the identification, collection, and transfer of information housed within that SharePoint site. Our collection focused on the SharePoint because I had identified it as the location of charged documents based upon the SIPRNET webpage address of those documents. Further, Special Agent (SA) John

Wilbur, with whom I was working, was interested in the contents of the USCENTCOM JAG folder.

4. The USCENTCOM SharePoint server is a tool to create an internet interface that allows users with access to the site on SIPRNET to collaborate, for example, by sharing files. The SharePoint itself is only accessible via SIPRNET, so a user must access it via secure systems. At that time, it was identified at IP addresses 131.240.47.23 (for the SharePoint database cluster), 131.240.47.6, and 131.240.47.7 (for the web portal front end or the portion accessible by SIPRNET users). The database as a whole occupied several terabytes of space. The server supporting it, from which I pulled the logs and other information at issue, is physically housed on virtual machines within a cluster, in a data center, on a storage area network (SAN). Only authorized USCENTCOM Headquarters J-6 personnel are granted access to the facility. The data center is protected by badge access, cipher locks, video surveillance, and an access roster.

5. The audit logs I referenced herein are Internet Information Systems (IIS) or Windows server log files, which capture the IP address of the USCENTCOM SharePoint server. The logs do not capture any remote or external IP addresses. The logs only capture the dates and times documents are accessed on the SharePoint server, as well as related activity on the SharePoint server.

6. For collection as evidence by SA Wilbur, these logs were pulled by the internet server maintenance team. I know this because I was there when they retrieved the information. These logs saved in a standard text file, or ".txt" format. I burned these logs onto a hard drive and also onto a DVD. I know these devices were clean of data because I personally wiped all information from the hard drive and laptop, and created the image for the hard drive on which the logs were burned. Further, I performed a hash value match to verify that the logs provided were saved accurately onto the disk. The DVD was red. I marked it with the title "CIE_USR_DATA". This DVD contained the files "CENTCOM_CIE_SharePoint-HASH_MD5SHA1.pdf", "CENTCOMHQ_CIE_SharePoint-HASH_MD5SHA1.txt", "web1.zip", and "web2.zip". The first two files contain the hash value information validating the accuracy of the log information collected. "Web1.zip" contained the weblog data from 1 December 2009 until 30 July 2010, pertaining to the USCENTCOM server assigned IP address 131.240.47.6. "Web2.zip" contained weblog data from 1 April 2010 until 30 July 2010, pertaining to the USCENTCOM server assigned to IP address 131.240.47.7. **Prosecution Exhibit 06 for Identification** are these SharePoint server logs.

7. After burning the log information to the DVD, I signed the evidence to SA Wilbur using the provided DA Form 4137 Evidence Property Custody Document. The disk was recorded on a DA Form 4137 labeled as document number (DN) 122-10. I recognize this as BATES number: 00411111. I know this because I signed that form and recognize my signature on it. I would recognize the evidence itself because I wrote the label on the disk and burned it. I did not alter the information or the devices on which it was housed in any way.

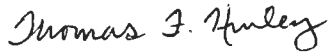
8. The information housed on the SharePoint server, mentioned previously, was accessed via SIPRNET and located in the JAG folder on the USCENTCOM SharePoint page. We collected this information for two reasons. First, collecting this information shows what content was

originally available on the USCENTCOM server to SIPRNET users. Second, this information helps put the log data we collected into context.

9. I assisted SA Wilbur in collecting this information from the SharePoint server. To retrieve it, we used two blank CCIU SATA hard drives. I know these are clear hard drives because, in accordance with USCENTCOM policy, I scanned them for malware and viruses before they were used to gather the evidence. Having found none, I knew they were suitable for evidence collection. To collect this information, we also used an approved CCIU laptop. I hooked this laptop to the SIPRNET using a CCIU-issued USB cable and drive dock. We then connected the previously scanned hard drive to the laptop. SA Wilbur used that connection to recover the information at issue.



ASHDEN FEIN
MAJ, JA
Trial Counsel



THOMAS F. HURLEY
MAJ, JA
Military Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused